有关 ASP的安全性问题的分析与研究

卢惟康

(厦门大学, 福建 厦门 361005)

摘 要: 本文阐述了 ASP的工作原理及 ASP网站一些基本的安全性问题和相关的解决办法。

关键词: 安全; 网站; ASP; IIS

一、前言

ASP (Active Server Pages) 是微软开发的基于 Windows NT server和 Internet Infomation Server的服务器脚本运行环境。它是一种高效的动态网页开发技术,使用它可以创建和运行动态、交互的 Web服务器应用程序。易于学习, 现在很多网站特别是电子商务方面的网站,在前台上大都用 ASP来实现。ASP是开发网站应用的快速工具,但是因为其使用的普遍性及源代码的开放性,使得其面临诸如数据被非法下载, 用户帐户泄露等一系列的安全问题。本文对代码本身的安全问题进行讨论。

二、ASP工作机理

(一) 运行 ASP所需的环境:

ASP的执行环境是在服务器端, 但并不是任何服务器都可以 ASP, ASP需要 Microsoft的 IIS (internet信息服务器) 或 PWS (个人 WEB服务器) 的支持。

(二) ASP工作机理

SP脚本是一系列按特定语法 (目前支持 VBscript和 JScript两种脚本语言) 编写的, 与标准 HTML页面混合在一起的脚本所构成的文本格式的文件。当客户端的最终用户用 WEB浏览器通过 INTERNET来访问基于 ASP脚本的应用时, WEB浏览器将向 WEB服务器发出 HTTP请求。WEB服务器分析、判断出该请求是 ASP脚本的应用后,自动通过 ISAPI接口调用 ASP脚本的解释运行引擎 (ASP.DLL)。ASP. DLL将从文件系统或内部缓冲区获取指定的 ASP脚本文件, 接着就进行语法分析并解释执行。最终的处理结果将形成 HTML格式的内容,通过 WEB服务器 "原路" 返回给 WEB浏览器, 由 WEB浏览器在客户端形成最终的结果呈现。这样就完成了一次完整的 ASP脚本调用。若干个有机的 ASP脚本调用就组成了一个完整的 ASP脚本应用。

三、ASP网站的主要安全问题及对策分析

ASP虽然具有易开发, 无需编译或连接即可执行, 无需客户端浏览器支持等许多优点, 但是我们也应该看到 ASP从一开始就一直受到众多漏洞的困扰, 比如: 源代码的泄露漏洞, 密码验证漏洞, IIS漏洞等。因此我们有必要了解 ASP所存在的安全问题,并且找到相应的对策, 使我们开发的 ASP网站更加安全可靠。

(一) ASP源代码的安全问题

从 ASP的原理上来看, ASP程序是在服务器端执行并解释成标准的 HTML文件再传送给客户端的浏览器, 一般的用户看不到 ASP的源代码, 但这并不是表示 ASP程序就绝对安全了。实际上 IIS本身的一些安全漏洞就可以查看到 ASP的源代码。比如, 在 IIS3 0以上就存在这样的漏洞, 在请求的 URL结尾加上某些特殊字符 (小数点, %81, ::$DATA等) 就可以看到 ASP的源代码; 再比如 IIS5 0的一个安全漏洞就是在 URL字符串的后面加上+ , HTM 就会导致某些 asa和 asp文件源

收稿日期: 2005- 10- 30

作者简介: 卢惟康 (1972-), 男, 江西萍乡人, 讲师, 研究方向: 计算机应用.

代码的泄露。别外 show code asp程序也可以看到 asp程序的源代码。除了上面列举的这些问题，利用 IIS的其它一些漏洞也可能导致 asp源代码的泄露，这里就不一一列举了。那么针对这些问题我们可以采取一些什么样的方法加以解决呢?首先要保证安装高版本的服务器软件，并及时安装相应的补丁程序，尽量避免这些漏洞的存在。其次是对 asp页面进行加密。加密的方法有两种，一种是采用组件技术将编程逻辑封装入 dll中。但是采用这种方法每段代码均需组件化，工作量较大。另一种加密方法就是使用微软的 script encoder对 asp页面进行加密。这种方法简单，效果也较好。Script encoder是免费软件，可以从微软的网站下载。

(二) ASP程序设计中的漏洞

使用 ASP 技术进行网站设计的一个主要目的就是 asp可以实现网站与浏览器之间的交互，而这也是形成漏洞的一大因素。比如在进行网上购物，查询或参与论坛，聊天，留言时，用户都需要填写一些数据，如果对这些数据没有进行充分的检查和验证，很可能造成网站服务器数据被破坏，更严重的还可能造成系统崩溃，因为 asp程序是在服务器端执行而 asp程序又要经常与网站目录，网站数据库这些敏感信息打交道，如果 asp程序设计中有漏洞，也就等于网站有漏洞。这时需要注意的问题就是在程序设计时对用户输入的数据进行全面的验证。因为用户输入什么样的值往往是不可以预见的，所以对这些信息的长度，内容，格式等都要进行充分的验证，才能避免错误的发生。尤其是对一些敏感字符，如 html标记，要充分过滤，避免形成页面炸弹。在程序设计时的另一个要注意的问题就是对用户合法性的验证。我们在网页设计时，往往在进入某些区域前都设置了登录页面，要求用户输入用户名和密码，以验证其合法性。但在实际应用中，有些非法用户往往可以使用所谓万能密码登录成功。这个漏洞产生的原因是程序设计时程序员把对用户名和密码的判断放在同一条语句中，而使用所谓万能密码就会使这个条件成立。针对这个问题程序设计者可以在验证用户名和密码是否正确之前先检查用户输入有无非法字符，如果有，立即转到错误页面。另外程序设计者也可以考虑修改程序，改变验证方式，先对用户名进行验证，如果通过再进行密码验证。除了上面的问题，还可能存在验证不全的问题。

(三) 数据库的安全问题

目前在许多使用 ASP技术的网站中都选择 access数据库作为数据存储的工具。在用 ACCESS做后台数据库时，如果有人通过各种方法知道或者猜到了服务器的 ACCESS数据库的路径和数据库名称，那么他能够下载这个 ACCESS数据库文件，这是非常危险的。比如：如果你的 ACCESS数据库 book.mdb放在虚拟目录下的 database目录下，那么有人在浏览器中打入：http：//someurl/database/book.mdb，如果你的 book.mdb数据库没有事先加密的话，那 book.mdb中所有重要的数据都掌握在别人的手中。

解决方法：

1. 为你的数据库文件名称起个复杂的非常规的名字，并把他放在几层目录下。所谓“非常规”，打个比方：

比如有个数据库要保存的是有关书籍的信息，可不要把他起个"book.mdb"的名字，起个怪怪的名称，比如 d34ksfslf.mdb，再把他放在如：/kdslf/i44/studi/的几层目录下，这样黑客要想通过猜的方式得到你的 ACCESS数据库文件就难上加难了。

2. 不要把数据库名写在程序中。有些人喜欢把 DSN 写在程序中，比如：DBPath = Server.MapPath(“cmddb.mdb”)

conn.Open“driver={Microsoft Access Driver(*.mdb)};dbq=”&DBPath，假如万一给人拿到了源程序，你的 ACCESS数据库的名字就一览无余。因此建议你在 ODBC里设置数据源，再在程序中这样写：conn open“shujiyuan”

3. 使用 ACCESS来为数据库文件编码及加密。首先在选取“工具→安全→加密/解密数据库”，选取数据库 (如：employer.mdb)，然后确定，接着会出现“数据库加密后另存为”的窗口，存为：employer1.mdb，接着 employer.mdb就会被编码，然后存为 employer1.mdb.，要注意的是，以上的动作并不是对数据库设置密码，而只是对数据库文件加以编码，目的是为了防止他人使用别的工具来查看数据库文件的内容。接下来我们为数据库加密，首先以打开经过编码了的 employer1.mdb，在打开时，选择“独占”方式。然后选取功能表的“工具→安全→设置数据库密码”，接着输入密码即可。为 employer1.mdb设置密码之后，接下来如果再使用 ACCEES数据库文件时，则 ACCESS会先要求输入密码，验证正确后才能够启动数据库。不过要在 ASP程序中的 connection对象的 open方法中增加 PWD的参数即可，例如：param=“driver={Microsoft Access Driver(*.mdb)};Pwd=yfdsfs”

(下转 117页)

计算机负责, 机房管理人员应详细记录每节课的机器使用情况. 这一教学常规已在我校计算机教师和学生中达成共识, 出现了问题马上可以追究相关人员的责任, 使得学生破坏系统的情况大大减少。为学校教学工作的正常运行提供了强有力的保障。

现在大力提供建设节约型社会, 学校机房也应本着“厉行节约, 讲究实效”的原则, 开展多媒体机房的“有序有偿开放”。所谓有序, 即利用学生的课余时间, 在教师的指导下, 有组织、有步骤参加各种实际应用能力考核培训, 制作多媒体计算机作品, 参加全国各种计算机竞赛, 以培养学生计算机应用能力和开发能力。所谓有偿, 根据上级有关文件精神, 使在双休日等非上课时间开放机房, 适当收取上机费用, 积累资金用于增加机房设备, 进一步完善机房条件, 起到“以机养机”的效果。这种“有序有偿开放”模式保持了机房较高的完发率和使用率, 为教学现代提供了有力的保障。

后话

机房管理是一种具有很强的专业性和很烦琐的工作。总结机房管理的经验, 目的就是为了更好的服务广大师生, 为正常的教育教学提供良好的后勤保障。以上只是我的个人经验, 免不了有错误和肤浅之处, 只是提供交流之用, 请大家多多指正和交流, 我们一起来探讨机房管理方法和各种技术, 把这项工作做好。

责任编辑: 彭利云

(上接 99页)

param= param&"; dbq= "&server. mappath ("employer1. mdb"), conn. open param

这样即使他人得到了 employer1. mdb文件, 没有密码他是无法看到 employer1. mdb的。

(四) FSO 对象对 WEB服务器数据安全的威胁

IIS 的 ASP 的文件操作都可以通过 FSO (file system object) 对象来实现, 包括文本文件的读写目录操作、文件的拷贝改名删除等, 但是这个强大的功能也留下了非常危险的 "后门"。利用 FSO (file system object) 对象可以篡改下载 FAT 分区上的任何文件。即使是 NTFS 分区, 如果权限没有设定好的话, 同样也能破坏, 一不小心你就可能遭受“灭顶之灾”。遗憾的是很多 webmaster只知道让 WEB服务器运行起来, 很少对 NTFS进行权限设置, 而 NT 目录权限的默认设置偏偏安全性又低得可怕。因此, 如果你是 Webmaster, 建议你密切关注服务器的设置, 尽量将 WEB目录建在 NTFS分区上, 目录不要设定 everyone full control, 即使是是管理员组的成员一般也没什么必要 full control, 只要有读取、更改权限就足够了。也可以把 FSO (file system object) 的组件删除或者改名。

四、结束语

ASP 是网站开发应用的一种快速工具, 但是我们不能只看到 ASP的快速开发能力, 而忽略了安全问题。本文只列举了一些较典型的安全问题, 要做到真正的安全, 需要有长期的实践经验并不断学习最新的安全知识。

参考文献:

[1]飞思科技产品研发中心. ASP& SQL Server网站设计与实现. 北京: 电子工业出版社 2001(1).

[2]刘瑞新、汪远征等. ASP网页数据库教程. 北京: 机械工业出版社 2004(1).

[3]求是科技. ASP 电子政务应用系统开发实例导航. 北京: 人民邮电出版社 2004(3).

[4]汪晓平, 钟军. ASP网络开发技术(第二版). 北京: 人民邮电出版社 2003(12).

责任编辑: 彭利云